Available online at www.sciencedirect.com

ScienceDirect

Finite Fields and Their Applications 14 (2008) 470–481

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

On value sets of polynomials over a field ☆

Zhi-Wei Sun

Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China

Received 8 March 2007; revised 8 May 2007

Available online 18 May 2007

Communicated by Rudolf Lidl

Abstract

Let F be any field. Let $p(F)$ be the characteristic of F if F is not of characteristic zero, and let $p(F)=+\infty$ otherwise. Let $A_1,\ldots,A_n$ be finite nonempty subsets of F, and let

$$f(x_1,\ldots,x_n)=a_1x_1^k+\cdots+a_nx_n^k+g(x_1,\ldots,x_n)\in F[x_1,\ldots,x_n]$$

with $k\in\{1,2,3,\ldots\}$, $a_1,\ldots,a_n\in F\setminus\{0\}$ and $\deg g<k$. We show that

$$\left|\left\{f(x_1,\ldots,x_n)\colon x_1\in A_1,\ldots,x_n\in A_n\right\}\right|\geqslant\min\left\{p(F),\sum_{i=1}^n\left\lfloor\frac{|A_i|-1}{k}\right\rfloor+1\right\}.$$

When $k\geqslant n$ and $|A_i|\geqslant i$ for $i=1,\ldots,n$, we also have

$$\begin{aligned}&\left|\left\{f(x_1,\ldots,x_n)\colon x_1\in A_1,\ldots,x_n\in A_n,\ \text{and } x_i\neq x_j \text{ if } i\neq j\right\}\right|\\&\quad\geqslant\min\left\{p(F),\sum_{i=1}^n\left\lfloor\frac{|A_i|-i}{k}\right\rfloor+1\right\};\end{aligned}$$

consequently, if $n\geqslant k$ then for any finite subset A of F we have

$$\left|\left\{f(x_1,\ldots,x_n)\colon x_1,\ldots,x_n\in A,\ \text{and } x_i\neq x_j \text{ if } i\neq j\right\}\right|\geqslant\min\left\{p(F),|A|-n+1\right\}.$$

☆ Supported by the National Science Fund (Grant No. 10425103) for Distinguished Young Scholars in China.

E-mail address: zwsun@nju.edu.cn.

URL: http://math.nju.edu.cn/~zwsun.

1071-5797/$ – see front matter

doi:10.1016/j.ffa.2007.05.002

In the case $n > k$, we propose a further conjecture which extends the Erdős–Heilbronn conjecture in a new direction.

Keywords: Value set; Polynomial; Field; Lower bound

1. Introduction

For a field F we use $p(F)$ to denote the additive order of the multiplicative identity of F, which is either infinite or a prime. A field F is said to have characteristic zero if $p(F) = +\infty$, and have characteristic p if $p(F)$ is a prime p.

By the Chevalley–Warning theorem (cf. [10, pp. 50–51]), for any polynomial $P(x_1, \ldots, x_n)$ over a finite field F, if $n > \deg P$ then the characteristic of F divides the number of solutions to the equation $P(x_1, \ldots, x_n) = 0$ over F^n. However, this says nothing about the solvability of the equation over F^n unless there is an obvious solution.

Given a field F, we consider polynomials of the form

$$f(x_1, \ldots, x_n) = a_1 x_1^k + \cdots + a_n x_n^k + g(x_1, \ldots, x_n) \in F(x_1, \ldots, x_n), \tag{1.1}$$

where

$$k \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}, \qquad a_1, \ldots, a_n \in F^* = F \setminus \{0\} \quad \text{and} \quad \deg g < k. \tag{1.2}$$

What can we say about the solvability of the equation $f(x_1, \ldots, x_n) = 0$ over F^n?

Let F be the field $F_p = \mathbb{Z}/p\mathbb{Z}$ with p a prime, and assume (1.1) and (1.2). In 1956 Carlitz [3] proved that the equation $f(x_1, \ldots, x_n) = 0$ has a solution in F_p^n when $k \mid p-1$ and $n \geqslant k$. In 2006 Felszeghy [7] extended this result by showing that the equation is solvable if $k < p$ and $n \geqslant \lceil (p-1)/\lfloor (p-1)/k \rfloor \rceil$. (For a real number α, $\lceil \alpha \rceil$ denotes the least integer not smaller than α while $\lfloor \alpha \rfloor$ represents the largest integer not exceeding α.) Note that the equation $f(x_1, \ldots, x_n) = 0$ over F_p^n is solvable if and only if the value set

$$\{ f(x_1, \ldots, x_n) \colon x_1, \ldots, x_n \in F_p \}$$

contains 0. In 1959 Chowla, Mann and Straus (cf. [10, pp. 60–61]) used Vosper's theorem (cf. [10, pp. 52–57]) to deduce that if $p > 3$, $1 < k < (p-1)/2$ and $k \mid p-1$, then

$$\left| \{ a_1 x_1^k + \cdots + a_n x_n^k \colon x_1, \ldots, x_n \in F_p \} \right| \geqslant \min \left\{ p, (2n-1)\frac{p-1}{k} + 1 \right\}.$$

Let F_q be the finite field of q elements where $q > 1$ is a prime power. In 1993 Wan, Shiue and Chen [14] showed that if $P(x)$ is a polynomial over F_q and $l \in \mathbb{N} = \{0, 1, 2, \ldots\}$ is the least nonnegative integer with $\sum_{x \in F_q} P(x)^l \neq 0$ then $|\{P(x) \colon x \in F_q\}| \geqslant l + 1$; in 2004 Das [4] extended this to multi-variable polynomials over F_q. By modifying the proof of [4, Theorem 1.5] slightly, one gets the following assertion: If $P(x_1, \ldots, x_n) \in F_q[x_1, \ldots, x_n]$, $\emptyset \neq S \subseteq F_q^n$, and l is the smallest nonnegative integer with $\sum_{(x_1, \ldots, x_n) \in S} P(x_1, \ldots, x_n)^l \neq 0$, then we have $|\{P(x_1, \ldots, x_n) \colon (x_1, \ldots, x_n) \in S\}| \geqslant l + 1$. Here the lower bound depends heavily on values of $P(x_1, \ldots, x_n)$.

In this paper we investigate two kinds of value sets of a polynomial in the form (1.1). Here is our first theorem which includes Felszeghy's result as a special case.

Theorem 1.1. *Let $f(x_1,\ldots,x_n)$ be a polynomial over a field F given by* (1.1) *and* (1.2). *Then, for any finite nonempty subsets $A_1,\ldots,A_n$ of F, we have*

$$\left|\left\{f(x_1,\ldots,x_n)\colon\ x_1\in A_1,\ldots,x_n\in A_n\right\}\right|\geqslant \min\left\{p(F),\ \sum_{i=1}^{n}\left\lfloor\frac{|A_i|-1}{k}\right\rfloor+1\right\}. \tag{1.3}$$

This result will be proved in Section 2 where we also give an example to show that the inequality (1.3) is sharp when F is an algebraically closed field.

Corollary 1.1 *(Cauchy–Davenport theorem). Let $A_1,\ldots,A_n$ be finite nonempty subsets of a field F. Then*

$$|A_1+\cdots+A_n|\geqslant \min\left\{p(F),|A_1|+\cdots+|A_n|-n+1\right\},$$

where the sumset $A_1+\cdots+A_n$ is given by

$$A_1+\cdots+A_n=\{x_1+\cdots+x_n\colon\ x_1\in A_1,\ldots,x_n\in A_n\}.$$

Proof. Simply apply Theorem 1.1 with $f(x_1,\ldots,x_n)=x_1+\cdots+x_n$. □

Remark 1.1. The original Cauchy–Davenport theorem (see [10, p. 44] or [13, p. 200]) is Corollary 1.1 in the case $n=2$ and $F=\mathbb{Z}/p\mathbb{Z}$ with p a prime.

Corollary 1.2. *Let F be a field of characteristic zero, and assume* (1.1) *and* (1.2). *Then, for any finite nonempty subset A of F, we have*

$$\left|\left\{f(x_1,\ldots,x_n)\colon\ x_1,\ldots,x_n\in A\right\}\right|\geqslant n\left\lfloor\frac{|A|-1}{k}\right\rfloor+1.$$

Proof. Just apply Theorem 1.1 with $A_1=\cdots=A_n=A$. □

Corollary 1.3. *Let F be a field with prime characteristic p, and let $f(x_1,\ldots,x_n)$ be given by* (1.1) *and* (1.2). *If A is a finite subset of F satisfying $\lfloor(|A|-1)/k\rfloor\geqslant(p-1)/n$, then*

$$\left|\left\{f(x_1,\ldots,x_n)\colon\ x_1,\ldots,x_n\in A\right\}\right|\geqslant p.$$

Proof. It suffices to apply Theorem 1.1 with $A_1=\cdots=A_n=A$. □

Remark 1.2. In the case $A=F=F_p$, Corollary 1.3 yields Felszeghy's result.

Now we state our second theorem.

Theorem 1.2. *Let $f(x_1,\ldots,x_n)$ be a polynomial over a field F given by* (1.1) *and* (1.2) *with $n\leqslant k=\deg f$. And let $A_1,\ldots,A_n$ be finite subsets of F with $|A_i|\geqslant i$ for $i=1,\ldots,n$. Then, for the restricted value set*

$$V=\big\{f(x_1,\ldots,x_n)\colon\ x_1\in A_1,\ldots,x_n\in A_n,\ \text{and } x_i\neq x_j \text{ if } i\neq j\big\},\tag{1.4}$$

we have

$$|V|\geqslant\min\left\{p(F),\ \sum_{i=1}^{n}\left\lfloor\frac{|A_i|-i}{k}\right\rfloor+1\right\}.\tag{1.5}$$

Corollary 1.4. *Let A be a finite subset of a field F, and let $f(x_1,\ldots,x_n)$ be a polynomial given by* (1.1) *and* (1.2). *Write $|A|=kq+r$ with $q,r\in\mathbb{N}$ and $r<k$. Then we have*

$$\begin{aligned}&\big|\big\{f(x_1,\ldots,x_n)\colon\ x_1,\ldots,x_n\in A,\ \text{and } x_i\neq x_j \text{ if } i\neq j\big\}\big|\\&\quad\geqslant\begin{cases}\min\{p(F),\ n(q-1)+\min\{n,r\}+1\} & \text{if } n\leqslant k,\\ \min\{p(F),\ |A|-n+1\} & \text{if } n\geqslant k.\end{cases}\end{aligned}\tag{1.6}$$

In Section 3 we shall prove Theorem 1.2 and Corollary 1.4, and give an example to illustrate that the inequality (1.5) is essentially best possible when F is an algebraically closed field.

In 1964 Erdős and Heilbronn [6] conjectured that if A is a subset of $\mathbb{Z}/p\mathbb{Z}$ with p a prime then

$$\big|\{x_1+x_2\colon\ x_1,x_2\in A\text{ and }x_1\neq x_2\}\big|\geqslant\min\big\{p,\ 2|A|-3\big\}.$$

Thirty years later this deep conjecture was confirmed by Dias da Silva and Hamidoune [5] who used the representation theory of groups to show that if A is a finite subset of a field F then

$$\begin{aligned}&\big|\{x_1+x_2+\cdots+x_n\colon\ x_1,\ldots,x_n\in A,\ \text{and } x_i\neq x_j \text{ if } i\neq j\}\big|\\&\quad\geqslant\min\big\{p(F),\ n\big(|A|-n\big)+1\big\}.\end{aligned}$$

This suggests that Corollary 1.4 in the case $n>k$ might be further improved. In Section 4 we will discuss our following conjecture which extends the Dias da Silva–Hamidoune result in a new way. (The reader may consult [2,8,9,12] for other generalizations of the Erdős–Heilbronn conjecture.)

Conjecture 1.1. *Let $f(x_1,\ldots,x_n)$ be a polynomial over a field F given by* (1.1) *and* (1.2), *and let A be any finite subset of F. Provided $n>k$, we have*

$$\begin{aligned}&\big|\big\{f(x_1,\ldots,x_n)\colon\ x_1,\ldots,x_n\in A,\ \text{and } x_i\neq x_j \text{ if } i\neq j\big\}\big|\\&\quad\geqslant\min\left\{p(F)-\delta,\ \frac{n(|A|-n)}{k}-k\left\{\frac{n}{k}\right\}\left\{\frac{|A|-n}{k}\right\}+1\right\},\end{aligned}\tag{1.7}$$

where $\{\alpha\}$ denotes the fractional part $\alpha-\lfloor\alpha\rfloor$ of a real number α, and

$$\delta=\begin{cases}1 & \text{if } n=2 \text{ and } a_1=-a_2,\\ 0 & \text{otherwise.}\end{cases}$$

2. Proof of Theorem 1.1

We need a useful tool of algebraic nature.

Combinatorial Nullstellensatz. *(See Alon [1].) Let $A_1, \ldots, A_n$ be finite subsets of a field F, and let $P(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$. Suppose that* $\deg P = k_1 + \cdots + k_n$ *where* $0 \leqslant k_i < |A_i|$ *for* $i = 1, \ldots, n$. *Then* $P(x_1, \ldots, x_n) \neq 0$ *for some* $x_1 \in A_1, \ldots, x_n \in A_n$ *if*

$$\left[x_1^{k_1} \cdots x_n^{k_n}\right] P(x_1, \ldots, x_n) \neq 0,$$

where $[x_1^{k_1} \cdots x_n^{k_n}]P(x_1, \ldots, x_n)$ *denotes the coefficient of* $x_1^{k_1} \cdots x_n^{k_n}$ *in* $P(x_1, \ldots, x_n)$.

Proof of Theorem 1.1. Let m be the largest nonnegative integer not exceeding n such that $\sum_{0<i\leqslant m} \lfloor (|A_i| - 1)/k \rfloor < p(F)$. For each $0 < i \leqslant m$ let A_i' be a subset of A_i with cardinality $k\lfloor (|A_i| - 1)/k \rfloor + 1$. In the case $m < n$, $p = p(F)$ is a prime and we let A_{m+1}' be a subset of A_{m+1} with

$$|A_{m+1}'| = k\left(p - 1 - \sum_{0<i\leqslant m} \left\lfloor \frac{|A_i| - 1}{k} \right\rfloor\right) + 1 < k\left\lfloor \frac{|A_{m+1}| - 1}{k} \right\rfloor + 1 \leqslant |A_{m+1}|.$$

If $m + 1 < j \leqslant n$ then we let $A_j' \subseteq A_j$ be a singleton. Whether $m = n$ or not, we have $\sum_{i=1}^n (|A_i'| - 1) = k(N - 1)$, where

$$N = \min\left\{p(F), \sum_{i=1}^n \left\lfloor \frac{|A_i| - 1}{k} \right\rfloor + 1\right\}.$$

Set

$$C = \left\{f(x_1, \ldots, x_n)\colon\ x_1 \in A_1', \ldots, x_n \in A_n'\right\}.$$

Suppose that $|C| \leqslant N - 1$. Then

$$\begin{aligned}
&\left[x_1^{|A_1'|-1} \cdots x_n^{|A_n'|-1}\right] f(x_1, \ldots, x_n)^{N-1-|C|} \prod_{c\in C} \big(f(x_1, \ldots, x_n) - c\big) \\
&\quad = \left[x_1^{|A_1'|-1} \cdots x_n^{|A_n'|-1}\right] \big(a_1 x_1^k + \cdots + a_n x_n^k\big)^{N-1} \\
&\quad = \frac{(N-1)!}{\prod_{i=1}^n ((|A_i'| - 1)/k)!} a_1^{(|A_1'|-1)/k} \cdots a_n^{(|A_n'|-1)/k} \neq 0.
\end{aligned}$$

By the Combinatorial Nullstellensatz, for some $x_1 \in A_1', \ldots, x_n \in A_n'$ we have

$$f(x_1, \ldots, x_n)^{N-1-|C|} \prod_{c\in C} \big(f(x_1, \ldots, x_n) - c\big) \neq 0$$

which contradicts the fact $f(x_1, \ldots, x_n) \in C$.

In view of the above,

$$\left|\left\{f(x_1,\ldots,x_n)\colon\ x_1\in A_1,\ldots,x_n\in A_n\right\}\right|\geqslant |C|\geqslant N$$

and this concludes the proof. □

Example 2.1. Let $a_1,\ldots,a_n\in F^*=F\setminus\{0\}$, where F is an algebraically closed field. For each $i=1,\ldots,n$ let

$$A_i=\left\{x\in F\colon\ f_k(x)\in\left\{a_i^{-1},2a_i^{-1},\ldots,q_ia_i^{-1}\right\}\right\}\setminus R_i,$$

where k and $q_i<p(F)$ are positive integers,

$$f_k(x)=\begin{cases}x^k-x & \text{if } p(F) \text{ is a prime divisor of } k,\\ x^k & \text{otherwise,}\end{cases}\tag{2.1}$$

and R_i is a subset of $\{x\in F\colon\ f_k(x)=q_ia_i^{-1}\}$ with $|R_i|=r_i\leqslant k-1$. For each $c\in F^*$, the equation $f_k(x)=c$ has exactly k distinct solutions in F since there is no $x\in F$ satisfying $f_k(x)-c=0=f_k'(x)$, where f_k' is the formal derivative of f_k. So $|A_i|=kq_i-r_i$ and hence

$$\left\lfloor\frac{|A_i|-1}{k}\right\rfloor=\left\lfloor\frac{k(q_i-1)+(k-1-r_i)}{k}\right\rfloor=q_i-1.$$

For every $i=1,\ldots,n$ we have

$$\left\{f_k(a)\colon\ a\in A_i\right\}=\left\{a_i^{-1},2a_i^{-1},\ldots,q_ia_i^{-1}\right\}.$$

Thus

$$\begin{aligned}&\left\{a_1f_k(x_1)+\cdots+a_nf_k(x_n)\colon\ x_1\in A_1,\ldots,x_n\in A_n\right\}\\&\quad=\left\{a_1\left(y_1a_1^{-1}\right)+\cdots+a_n\left(y_na_n^{-1}\right)\colon\ y_i\in\{1,\ldots,q_i\}\text{ for }i=1,\ldots,n\right\}\\&\quad=\left\{(y_1+\cdots+y_n)e\colon\ y_i\in\{1,\ldots,q_i\}\text{ for }i=1,\ldots,n\right\}\\&\quad=\left\{ne,(n+1)e,\ldots,(q_1+\cdots+q_n)e\right\},\end{aligned}$$

where e denotes the multiplicative identity of the field F. Observe that

$$q_1+\cdots+q_n-n=\sum_{i=1}^n(q_i-1)=\sum_{i=1}^n\left\lfloor\frac{|A_i|-1}{k}\right\rfloor.$$

Therefore

$$\begin{aligned}&\left|\left\{a_1f_k(x_1)+\cdots+a_nf_k(x_n)\colon\ x_1\in A_1,\ldots,x_n\in A_n\right\}\right|\\&\quad=\min\left\{p(F),\ \sum_{i=1}^n\left\lfloor\frac{|A_i|-1}{k}\right\rfloor+1\right\}.\end{aligned}$$

3. Proofs of Theorem 1.2 and Corollary 1.4

Proof of Theorem 1.2. Let $q_i = \lfloor (|A_i| - i)/k \rfloor$ for $i = 1, \ldots, n$. And let m be the largest non-negative integer not exceeding n such that $\sum_{0<i\leqslant m} q_i < p(F)$. For each $0 < i \leqslant m$ let A'_i be a subset of A_i with cardinality $kq_i + i$. In the case $m < n$, $p = p(F)$ is a prime and we let A'_{m+1} be a subset of A_{m+1} with

$$|A'_{m+1}| = k\biggl(p - 1 - \sum_{0<i\leqslant m} q_i\biggr) + m + 1 < kq_{m+1} + m + 1 \leqslant |A_{m+1}|.$$

If $m + 1 < j \leqslant n$ then we let $A'_j \subseteq A_j$ with $|A_j| = j$. Whether $m = n$ or not, we have $\sum_{i=1}^{n}(|A'_i| - i) = k(N - 1)$, where

$$N = \min\bigl\{p(F),\ q_1 + \cdots + q_n + 1\bigr\}.$$

Set

$$C = \bigl\{f(x_1, \ldots, x_n)\colon\ x_1 \in A'_1, \ldots, x_n \in A'_n,\ \text{and } x_i \neq x_j \text{ if } i \neq j\bigr\}.$$

Suppose that $|C| \leqslant N - 1$ and let $P(x_1, \ldots, x_n)$ denote the polynomial

$$f(x_1, \ldots, x_n)^{N-1-|C|} \prod_{c\in C}\bigl(f(x_1, \ldots, x_n) - c\bigr) \prod_{1\leqslant i<j\leqslant n}(x_j - x_i).$$

Then

$$\deg P \leqslant k(N - 1) + \binom{n}{2} = \sum_{i=1}^{n}\bigl(|A'_i| - 1\bigr).$$

By linear algebra,

$$\prod_{1\leqslant i<j\leqslant n}(x_j - x_i) = \det\bigl(x_i^{j-1}\bigr)_{1\leqslant i,j\leqslant n} = \sum_{\sigma\in S_n} \operatorname{sign}(\sigma) \prod_{i=1}^{n} x_i^{\sigma(i)-1},$$

where S_n is the symmetric group of all permutations on $\{1, \ldots, n\}$, and $\operatorname{sign}(\sigma)$ is 1 or -1 according as σ is even or odd. Recall that

$$|A'_i| = \begin{cases} kq_i + i & \text{if } 1 \leqslant i \leqslant m, \\ k(p(F) - 1 - q_1 - \cdots - q_m) + i & \text{if } i = m + 1 \leqslant n, \\ i & \text{if } m + 1 < i \leqslant n. \end{cases}$$

For each $i = 1, \ldots, n$, we clearly have $|A'_i| - 1 \equiv i - 1 \pmod{k}$ and $\sigma(i) - 1 < n \leqslant k$ for all $\sigma \in S_n$. Thus

$$\begin{aligned}
&\big[x_1^{|A_1'|-1}\cdots x_n^{|A_n'|-1}\big]P(x_1,\ldots,x_n)\\
&\quad=\big[x_1^{|A_1'|-1}\cdots x_n^{|A_n'|-1}\big]\big(a_1x_1^k+\cdots+a_nx_n^k\big)^{N-1}\sum_{\sigma\in S_n}\operatorname{sign}(\sigma)\prod_{i=1}^n x_i^{\sigma(i)-1}\\
&\quad=\left[\prod_{i=1}^n x_i^{|A_i'|-1}\right]\sum_{j_1+\cdots+j_n=N-1}\frac{(N-1)!}{j_1!\cdots j_n!}a_1^{j_1}\cdots a_n^{j_n}\prod_{i=1}^n x_i^{j_ik+i-1}\\
&\quad=\frac{(N-1)!}{q_1!\cdots q_m!q!}a_1^{q_1}\cdots a_m^{q_m}a\neq 0,
\end{aligned}$$

where $q=a=1$ if $m=n$, and $q=(p(F)-1-q_1-\cdots-q_m)!$ and $a=a_{m+1}^q$ if $m<n$. In light of the Combinatorial Nullstellensatz, there are $x_1\in A_1',\ldots,x_n\in A_n'$ such that $P(x_1,\ldots,x_n)\neq 0$. Obviously this contradicts the fact $f(x_1,\ldots,x_n)\in C$.

By the above, $|V|\geqslant|C|\geqslant N$ and hence (1.5) holds. □

Example 3.1. Let F be any algebraically closed field, and let $a_1,\ldots,a_n\in F^*$. For each $i=1,\ldots,n$ let

$$A_i=S_i\cup\big\{x\in F:\ f_k(x)\in\big\{ja_i^{-1}:\ 1<j\leqslant q_i\big\}\big\},$$

where $k\geqslant n$ and $q_i<p(F)$ are positive integers, $f_k(x)$ is given by (2.1), and S_i is a subset of $\{x\in F:\ f_k(x)=a_i^{-1}\}$ with $|S_i|\geqslant i$. Observe that $|A_i|=k(q_i-1)+|S_i|$ and hence

$$\left\lfloor\frac{|A_i|-i}{k}\right\rfloor=q_i-1.$$

For every $i=1,\ldots,n$, we have

$$\big\{f_k(a):\ a\in A_i\big\}=\big\{a_i^{-1},2a_i^{-1},\ldots,q_ia_i^{-1}\big\}.$$

If $y_i\in\{1,\ldots,q_i\}$ for $i=1,\ldots,n$, we can find distinct $x_1\in A_1,\ldots,x_n\in A_n$ such that $f_k(x_i)=y_ia_i^{-1}$ for $i=1,\ldots,n$; in fact, if $x_1\in A_1,\ldots,x_{i-1}\in A_{i-1}$ are distinct with $i\leqslant n$, and $f_k(x_j)=y_ja_j^{-1}$ for $j=1,\ldots,i-1$, then we can choose $x_i\in A_i\setminus\{x_1,\ldots,x_{i-1}\}$ satisfying $f_k(x_i)=y_ia_i^{-1}$ because $k\geqslant|S_i|>i-1$. Thus

$$\begin{aligned}
&\big\{a_1f_k(x_1)+\cdots+a_nf_k(x_n):\ x_1\in A_1,\ldots,x_n\in A_n,\ \text{and } x_i\neq x_j \text{ if } i\neq j\big\}\\
&\quad=\big\{a_1\big(y_1a_1^{-1}\big)+\cdots+a_n\big(y_na_n^{-1}\big):\ y_i\in\{1,\ldots,q_i\}\text{ for }i=1,\ldots,n\big\}\\
&\quad=\big\{(y_1+\cdots+y_n)e:\ y_i\in\{1,\ldots,q_i\}\text{ for }i=1,\ldots,n\big\}\\
&\quad=\big\{ne,(n+1)e,\ldots,(q_1+\cdots+q_n)e\big\},
\end{aligned}$$

where e is the multiplicative identity of F. Note that

$$q_1+\cdots+q_n-n=\sum_{i=1}^n(q_i-1)=\sum_{i=1}^n\left\lfloor\frac{|A_i|-i}{k}\right\rfloor.$$

So we have

$$\begin{aligned}&\big|\big\{a_1 f_k(x_1)+\cdots+a_n f_k(x_n)\colon\ x_1\in A_1,\ldots,x_n\in A_n,\ \text{and } x_i\neq x_j \text{ if } i\neq j\big\}\big|\\&\quad=\min\bigg\{p(F),\ \sum_{i=1}^n\bigg\lfloor\frac{|A_i|-i}{k}\bigg\rfloor+1\bigg\}.\end{aligned}$$

Proof of Corollary 1.4. The case $|A|<n$ is trivial; below we assume $|A|\geqslant n$.

We first handle the case $n\leqslant k$. If $1\leqslant i\leqslant\min\{n,r\}$ then we let A_i be a subset of A with cardinality $kq+i+\max\{r-n,0\}\leqslant kq+r=|A|$; if $r<j\leqslant n$ then we let A_j be a subset of A with cardinality $k(q-1)+j\leqslant k(q-1)+n\leqslant kq$. (Note that when $r<n$ we have $q\neq 0$ since $|A|\geqslant n$.) Obviously,

$$\sum_{i=1}^n\bigg\lfloor\frac{|A_i|-i}{k}\bigg\rfloor=\sum_{i=1}^{\min\{n,r\}}q+\sum_{r<j\leqslant n}(q-1)=n(q-1)+\min\{n,r\}.$$

Applying Theorem 1.2 we obtain that

$$\begin{aligned}&\big|\big\{f(x_1,\ldots,x_n)\colon\ x_1,\ldots,x_n\in A,\ \text{and } x_i\neq x_j \text{ if } i\neq j\big\}\big|\\&\quad\geqslant\big|\big\{f(x_1,\ldots,x_n)\colon\ x_1\in A_1,\ldots,x_n\in A_n,\ \text{and } x_i\neq x_j \text{ if } i\neq j\big\}\big|\\&\quad\geqslant\min\big\{p(F),\ n(q-1)+\min\{n,r\}+1\big\}.\end{aligned}$$

In particular, if $k=n$ then

$$\begin{aligned}&\big|\big\{f(x_1,\ldots,x_n)\colon\ x_1,\ldots,x_n\in A,\ \text{and } x_i\neq x_j \text{ if } i\neq j\big\}\big|\\&\quad\geqslant\min\big\{p(F),\ n(q-1)+r+1\big\}=\min\big\{p(F),\ |A|-n+1\big\}.\end{aligned}$$

Now suppose that $n>k$. Let $c_{k+1},\ldots,c_n$ be $n-k$ distinct elements of A. Then $A'=A\setminus\{c_{k+1},\ldots,c_n\}$ has cardinality $|A|-(n-k)$. By what we have proved,

$$\begin{aligned}&\big|\big\{f(x_1,\ldots,x_k,c_{k+1},\ldots,c_n)\colon\ x_1,\ldots,x_k\in A',\ \text{and } x_i\neq x_j \text{ if } i<j\big\}\big|\\&\quad\geqslant\min\big\{p(F),\ |A'|-k+1\big\}=\min\big\{p(F),\ |A|-n+1\big\}.\end{aligned}$$

So the desired inequality follows. □

4. Discussion of Conjecture 1.1

Conjecture 1.1 in the case $f(x_1,\ldots,x_n)=x_1+\cdots+x_n$, essentially gives the Dias da Silva–Hamidoune result mentioned in Section 1.

In the case $f(x_1,\ldots,x_n)=x_1^k+\cdots+x_n^k$ with $k>1$, we may explain the symmetry between n and $|A|-n$ as follows. If $|A|>n$ then

$$\begin{aligned}&\left|\left\{x_1^k+\cdots+x_n^k\colon\ x_1,\ldots,x_n\in A,\ \text{and } x_i\neq x_j \text{ if } i\neq j\right\}\right|\\&\quad=\left|\left\{\sum_{a\in A}a^k-y_1^k-\cdots-y_{|A|-n}^k\colon\ y_1,\ldots,y_{|A|-n}\in A,\ \text{and } y_i\neq y_j \text{ if } i\neq j\right\}\right|\\&\quad=\left|\left\{y_1^k+\cdots+y_{|A|-n}^k\colon\ y_1,\ldots,y_{|A|-n}\in A,\ \text{and } y_i\neq y_j \text{ if } i\neq j\right\}\right|.\end{aligned}$$

Conjecture 1.1 holds when $n=2$. In fact, if we set $A_1=\{a_1x\colon\ x\in A\}$ and $A_2=\{a_2x\colon\ x\in A\}$, then $|A_1|+|A_2|-3=2(|A|-2)+1$ and

$$\begin{aligned}&\left|\left\{a_1x_1+a_2x_2\colon\ x_1,x_2\in A \text{ and } x_1\neq x_2\right\}\right|\\&\quad=\left|\left\{y_1+y_2\colon\ y_1\in A_1,\ y_2\in A_2 \text{ and } a_1^{-1}y_1\neq a_2^{-1}y_2\right\}\right|\\&\quad=\left|\left\{y_1+y_2\colon\ y_1\in A_1,\ y_2\in A_2 \text{ and } y_1-a_1a_2^{-1}y_2\neq 0\right\}\right|\\&\quad\geqslant\min\left\{p(F)-\delta,\ |A_1|+|A_2|-3\right\}\quad[11,\text{ Corollary 3}].\end{aligned}$$

The following example illustrates how the lower bound in (1.7) comes out.

Example 4.1. Let $k,n\in\mathbb{Z}^+$ and $q\in\mathbb{N}$. Let

$$A=\left\{z\in\mathbb{C}\colon\ z^k\in\{1,\ldots,q\}\right\}\cup R,$$

where $\mathbb{C}$ is the field of complex numbers and R is a subset of $\{z\in\mathbb{C}\colon\ z^k=q+1\}$ with cardinality $r<k$. Suppose that $n\geqslant k$ and $|A|=kq+r\geqslant n=k\lfloor n/k\rfloor+s$ with $s\in\{0,\ldots,k-1\}$. Clearly,

$$V=\left\{x_1^k+\cdots+x_n^k\colon\ x_1,\ldots,x_n\in A,\ \text{and } x_i\neq x_j \text{ if } i\neq j\right\}$$

just consists of those sums $\sum_{i=1}^n y_i$ with $y_i\in\{1,\ldots,q+1\}$, $|\{i\colon\ y_i=q+1\}|\leqslant r$ and $|\{i\colon\ y_i=j\}|\leqslant k$ for all $j=1,\ldots,q$. Thus the smallest element of V is

$$m_V=k\sum_{i=1}^{\lfloor n/k\rfloor}i+s\left(\left\lfloor\frac{n}{k}\right\rfloor+1\right)=\left(\frac{k}{2}\left\lfloor\frac{n}{k}\right\rfloor+s\right)\left(\left\lfloor\frac{n}{k}\right\rfloor+1\right),$$

while the largest element of V is

$$M_V=r(q+1)+k\sum_{i=0}^{\lfloor n/k\rfloor-1}(q-i)+(s-r)\left(q-\left\lfloor\frac{n}{k}\right\rfloor\right)-d(r,s),$$

where

$$d(r,s)=\begin{cases}r-s & \text{if } r\geqslant s,\\ 0 & \text{if } r<s.\end{cases}$$

It follows that

$$\begin{aligned}
&d(r,s)+M_V-m_V\\
&\quad=r(q+1)+kq\left\lfloor\frac{n}{k}\right\rfloor-k\left\lfloor\frac{n}{k}\right\rfloor^2+(s-r)q+(r-s)\left\lfloor\frac{n}{k}\right\rfloor-s\left(\left\lfloor\frac{n}{k}\right\rfloor+1\right)\\
&\quad=\left\lfloor\frac{n}{k}\right\rfloor\left(kq+r-s-k\left\lfloor\frac{n}{k}\right\rfloor-s\right)+r+sq-s\\
&\quad=\left\lfloor\frac{n}{k}\right\rfloor\big(|A|-s-n\big)+s(q-1)+r\\
&\quad=\left\lfloor\frac{n}{k}\right\rfloor\big(|A|-n\big)+s\left(q-\left\lfloor\frac{n}{k}\right\rfloor-1\right)+r\\
&\quad=\left\lfloor\frac{n}{k}\right\rfloor\big(|A|-n\big)+s\left\lfloor\frac{|A|-n}{k}\right\rfloor+\begin{cases}r-s & \text{if } r\geqslant s,\\ r & \text{if } r<s.\end{cases}
\end{aligned}$$

Therefore

$$\begin{aligned}
|V|&=\big|\{m_V,\dots,M_V\}\big|=M_V-m_V+1\\
&=1+\left\lfloor\frac{n}{k}\right\rfloor\big(|A|-n\big)+s\left\lfloor\frac{|A|-n}{k}\right\rfloor+\begin{cases}r & \text{if } r<s,\\ 0 & \text{otherwise.}\end{cases}
\end{aligned}$$

Finally, we note that

$$\begin{aligned}
\left\lfloor\frac{n}{k}\right\rfloor\big(|A|-n\big)+s\left\lfloor\frac{|A|-n}{k}\right\rfloor&=\left(\frac{n}{k}-\left\{\frac{n}{k}\right\}\right)\big(|A|-n\big)+k\left\{\frac{n}{k}\right\}\left\lfloor\frac{|A|-n}{k}\right\rfloor\\
&=\frac{n(|A|-n)}{k}-k\left\{\frac{n}{k}\right\}\left\{\frac{|A|-n}{k}\right\}.
\end{aligned}$$

Acknowledgments

The author thanks the referees for their helpful comments.

References

[1] N. Alon, Combinatorial Nullstellensatz, Combin. Probab. Comput. 8 (1999) 7–29.
[2] N. Alon, M.B. Nathanson, I.Z. Ruzsa, The polynomial method and restricted sums of congruence classes, J. Number Theory 56 (1996) 404–417.
[3] L. Carlitz, Solvability of certain equations in a finite field, Quart. J. Math. 7 (1956) 3–4.
[4] P. Das, Value sets of polynomials and the Cauchy–Davenport theorem, Finite Fields Appl. 10 (2004) 113–122.
[5] J.A. Dias da Silva, Y.O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, Bull. London Math. Soc. 26 (1994) 140–146.
[6] P. Erdős, H. Heilbronn, On the addition of residue classes modulo p, Acta Arith. 9 (1964) 149–159.
[7] B. Felszeghy, On the solvability of some special equations over finite fields, Publ. Math. Debrecen 68 (2006) 15–23.
[8] Q.H. Hou, Z.W. Sun, Restricted sums in a field, Acta Arith. 102 (2002) 239–249.
[9] G. Károlyi, The Erdős–Heilbronn problem in abelian groups, Israel J. Math. 139 (2004) 349–359.
[10] M.B. Nathanson, Additive Number Theory: Inverse Problems and the Geometry of Sumsets, Grad. Texts in Math., vol. 165, Springer, New York, 1996.
[11] H. Pan, Z.W. Sun, A lower bound for $|\{a+b: a\in A, b\in B, P(a,b)\neq 0\}|$, J. Combin. Theory Ser. A 100 (2002) 387–393.

[12] Z.W. Sun, On Snevily's conjecture and restricted sumsets, J. Combin. Theory Ser. A 103 (2003) 288–301.
[13] T. Tao, V.H. Vu, Additive Combinatorics, Cambridge Univ. Press, Cambridge, 2006.
[14] D. Wan, P.J.-S. Shiue, C.S. Chen, Value sets of polynomials over finite fields, Proc. Amer. Math. Soc. 119 (1993) 711–717.